UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/611,809	07/07/2000	David K. Chin	BRCMP002	6867

7590 03/21/2005

CHRISTIE, PARKER & HALE
P.O. BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
COLIN, CARL G	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/611,809	CHIN ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 January 2005* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 July 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 1/3/2005 for request to continue examination, applicant amends claims 1, 2, 3, and adds claims 21 and 22. The following claims 1-22 are presented for examination.

2. Applicant's arguments, pages 8-9, filed on 12/23/2003, with respect to the rejection of claims 1-20 have been fully considered, and they are persuasive as amended. Applicant argues that Hobson does not teach or suggest the use of instructions to cause specified operations to be performed in parallel. Examiner respectfully disagrees because Hobson suggests in column 8, lines 28-30 that the control of the sequence can be under software control using the CPU. Applicant amends claim 1 and adds claims 21-22 to further limit the claimed invention. Upon further consideration a new ground of rejection is made in view of Hobson and Fisher. Claims 1-22 are now rejected under 35 USC 103 (a) in view of Hobson and Fisher.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have

been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3.1 **Claims 1-6 and 9-22** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,209,016 to **Hobson et al.** in view of US Patent 6,237,016 to **Fisher et al**.

3.2 **As per claims 1, 2, 3, 21, and 22, Hobson et al.** substantially teaches an apparatus and method comprising: an encryption processor (see figure 2) including: an execution unit configured to execute product and square operations, the execution unit including at least one adder and at least two multipliers (see figures 3-4). **Hobson et al.** discloses a decode unit in figure 6 that meets the recitation of a decode unit coupled to an instruction unit being configured to determine if a square operation or a product operation needs to be performed on an operand (see column 6, lines 44-49). **Hobson et al.** teaches performing multiplication and addition operations in parallel to improve performance time (see column 4, lines 27-40 and claim 7). **Hobson et al.** further suggests using instruction to control operations (column 8, lines 28-30 and column 1, lines 40-50). **Fisher et al** in an analogous art teaches a decode unit and execution unit for performing instructions and a decode unit issuing instructions to perform specific operations (column 7, lines 23-33). **Fisher et al** further discloses first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication-addition operations (see column 8, lines 12-41) one multiplication-addition operation can also be performed at one time in another embodiment (column 9, lines 6-8). **Fisher et al** adds that one

of the advantages of this technique is to improve performance in performing complex calculations, for example only two instructions are needed in performing complex multiplication operations (column 6, lines 4-16). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the method of **Hobson** of determining whether to perform a Montgomery square operation or a Montgomery product operation in parallel and performing either the Montgomery square or Montgomery multiplication with the method of **Fisher et al** of issuing specific instruction to perform simultaneous multiplication operations and specific instruction to perform simultaneous multiplication and addition operations to provide a decoder unit issuing instructions comprising a first instruction to perform simultaneous multiplication operations and second instruction to perform simultaneous multiplication and addition operations in performing a square and an additional third instruction to perform simultaneous multiplication and addition operations in performing a multiplication as taught by **Fisher et al**. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Fisher et al** so as to improve performance in performing calculations with fewer decoding instructions (column 9, lines 38-45).

As per claim 4, Hobson et al. discloses the limitation of wherein certain of the multiplication operations are performed in parallel using a multiply and shift (see column 2, lines 19-49). It is apparent to one skill in the art that certain of the multiplication operations can be processed in parallel as mentioned above by one instruction.

As per claim 5, Hobson et al. discloses the limitation of wherein the execution unit further comprises registers coupled to the multiplication units and the at least one adder (see figure 1).

As per claim 6, Hobson et al. discloses the limitation of wherein the encryption processor further comprises a memory coupled to the execution unit and the decode unit (see figure 6).

As per claims 9-11, Hobson et al. discloses a co-processor for performing modular multiplication and Montgomery algorithm. It is well known in the art that the integrated circuit disclosed herein can be incorporated in a server and used to establish a secure socket layer connection between the server and a client; and embedded in a microprocessor within the server; and contained on a dedicated processor which is coupled via a bus to a microprocessor in the server.

As per claims 12 and 13, Hobson et al. discloses the limitation of wherein the product and square operations executed by the execution unit are Montgomery product and square operations wherein the product and square operations are performed on operands having at least one of the following widths: 256 bits wide; 512 bits wide; 768 bits wide; 1,024 bits wide; 1536 bits wide; 2,048 bits wide; 3072 bits wide; 4,096 bits wide; 8,192 bits wide; 16,384 bits wide; 32,768 bits wide; or 65,536 bits wide (see column 1, lines 5-8 and column 2, lines 14-18).

As per claims 14-20, Hobson et al. substantially discloses a co-processor. It is known in the art hardware/software technologies that support encryption processor. Official notice is taken by examiner that it would have been obvious to have the encryption processor configured into a secure web server or a secure switch or internet load balance device deploying SSL/TLS or router or VPN gateways or remote access devices used for VPN applications. **Hobson et al.** does not disclose a secure switch deploying Secure Socket Layer (SSL)/Transport Layer Security (TLS). This modification would have been obvious because one skilled in the art would have been motivated to implement the encryption processor into the examples above to establish network security and take advantage of the processor speed in performing Montgomery calculation.

4. **Claims 7-8** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,209,016 to **Hobson et al.** in view of US Patent 6,237,016 to **Fisher et al** as applied to claim 1 and further in view of US Patent 6,064,740 to **Curiger et al.**.

4.1 **As per claims 7 and 8, Hobson et al.** discloses the limitation of wherein the decode unit is further configured to decode an operation $M=C^d \bmod N$ and discloses determining whether to perform a square or multiply; and if the exponent d equals to a first logic state implement a square and a product operation. **Hobson et al.** does not explicitly teach the details of the process. However, **Curiger et al.** in an analogous art teaches (a) determining the MSB position of the exponent d equal to a first logic state and (b) issuing a first set of instructions to implement a square and a product operation after the MSB position of the exponent d equal to a first logic

state is determined (see column 11, lines 3-9); (c) determining if the next most significant bit (MSB) of exponent (d) is the first digital state or a second digital state; and either (d) issuing a second set of instructions to the execution unit to implement a square operation if the next MSB is of the second digital state; or (e) issuing the first set of instructions to the execution unit if the next MSB of the exponent is of the first digital state instructions to implement a square and a product operation (see column 11, lines 9-15); and repeating (c) through (e) for every bit in the exponent (d) from the next MSB to the least significant bit (LSB) (see column 11, lines 15-25). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method and apparatus as combined above to apply the instructions as described above and the final result of the operation $M = C^d \bmod N$ by accumulating the results of (b) through (e) as taught by **Curiger et al.** to maximize the speed of the calculations. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Curiger et al.** so as to maximize the speed of the calculations.

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Carl Colin
Patent Examiner
March 10, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100